Information Technology Security Policy

Carmella Thompson

State of Maryland Information Technology Security & Privacy Conference 2003

September 24 & 25, 2003

Information Technology Security Policy

- Provides policy and supporting standards for information technology security.
- The policy applies to Executive agencies of the State of Maryland.
- The responsibility for each agency to have its own technology security plan.
- The standards establish minimum levels of compliance.
- The policy covers such common technologies as computers, data and voice networks, wireless systems, web systems, and many other more specialized resources.

Information Technology Security Policy

- The statewide program based on this policy provides the minimum requirements and a consistent approach for security.
- The common security approach also supports compatible security solutions shared among agencies, yielding a better return on technology investment.
- The security policy and standards will evolve and will require regular updates to remain current.

Information Technology Security Policy

- Information and information technology systems are essential assets of the State of Maryland. They are vital to the citizens of the State. Information assets are critical to the services that agencies provide to citizens, businesses, and educational institutions, as well as, to local and federal government entities and to other State agencies. All information created with State resources for State operations is the property of the State of Maryland. All agencies, employees, and contractors of the State are responsible for protecting information from unauthorized access, modification, disclosure and destruction.

Information Technology Security Policy

- Each agency of the Executive Branch of the State is responsible for compliance with this policy and these standards. The Office of Information Technology (OIT) of the Department of Budget and Management and agency Information Technology (IT) components are to use this policy and these standards as a guide when procuring information technology services, service providers, contractors, software, hardware and network components.

Information Technology Security Policy Scope

- This policy covers all information that is electronically generated, received, stored, printed, filmed, and typed. In accordance with the Annotated Code of Maryland, State Finance and Procurement Article, Section 3-401 through 3-413 and Section 3-701 through 3-705, and with the Executive Order 01.01.1983.18 Privacy and State Data System Security Paragraph 4.D, the provisions of this policy apply to:
  - □ • All units of the Executive Branch of the State of Maryland for all of their IT systems regardless of who is operating them
  - □ • All activities and operations required to ensure data security including facility design, physical security, disaster recovery and business continuity planning, use of hardware and operating systems or application software, data disposal, and protection of copyrights and other intellectual property rights

Information Technology Security Policy

Objectives

- To establish a secure environment for the processing of data

- To reduce information security risk

- To communicate the responsibilities for the protection of information

Information Technology Security Policy Compliance

- The head of each agency is responsible for compliance with and enforcement of this Policy.

- Agency Chief Information Officers (CIOs) shall develop and implement an Agency IT Security Program to implement this policy and these standards. The Security Program shall include a timetable and controls for compliance. The controls shall include but are not limited to:
  - Maintaining the confidentiality, integrity, availability, and accountability of all State information technology applications and services
  - Protecting information according to its sensitivity, criticality and value, regardless of the media on which it is stored or automated systems that process it, or the methods by which it is distributed

Information Technology Security Policy Compliance

- The controls shall include but are not limited to:
  - Ensuring that risks to information security are identified and controls implemented to mitigate these risks
  - Implementing processes to ensure that all security services meet the minimum requirements set forth in this policy and the attached standards
  - Ensuring that all employees and contractors understand and comply with this Policy, as well as all applicable laws and regulations
  - Implementing physical security controls to prevent unauthorized and/or illegal access, misuse, destruction or theft of the State’s IT assets

Information Technology Security Policy
Security Program Maintenance and Review

- Each State agency will review and update its IT Security Program as needed to conform to changes within the agency or in the State IT Security Program. IT Systems security plans will be reviewed as required by IT security Certification and Accreditation guidelines.

Information Technology Security Policy Deviation and Risk Acceptance

- Compliance with this policy shall be planned and achieved as promptly as possible.

- When an agency determines that it is not feasible or practical to comply with a provision or provisions of this policy and attendant standards, or to do so promptly, it shall document the deviation from policy or standards.

- The documentation, with a timetable for compliance when practicable, shall be prepared as an IT Security Deviation Request.

Information Technology Security Policy Deviation and Risk Acceptance

- **IT Security Deviation Requests must be filed in accordance with the specifications detailed in the State IT Security Deviation/Risk Acceptance Standard**

  – Such deviations require the approval of the agency CIO and the State CIO.

Information Technology Security Policy

Security Program Standard

- **At a minimum each program must contain the following elements:**

  - **IT Security Policy**
  - **Risk Management**
  - **Systems Development Life Cycle Methodology**
  - **IT Security Certification and Accreditation**
  - **IT Disaster Recovery Planning**
  - **IT Security Awareness Training**
  - **IT Incident Response Process**
  - **External Connections Review**
  - **IT Security Plan Reporting.**

- **4.7 IT Incident Response Process**

Agencies shall be required to participate in the State Incident Response Process by detecting, tracking, logging, and reporting security incidents. (See the Maryland Computer Incident Response Capability Procedures and the Standard Operation Procedures for Electronic Evidence Handling)

Information Technology Security Policy

Security Program Standard

- **4.8 IT Incident Response Process**

External network connections, non-networked computers and dial-in connections shall be managed, reviewed annually, and documented as prescribed by the Agency IT Security Program. Results will be reported annually as part of the IT security assessment transmitted to the Office of the State CIO and to the SDSC

Information Technology Security Policy

Security Program Standard

4.9 IT Security Plan Reporting

– Each agency is responsible for reporting on the status of the agency IT Security Program to the State Data Security Committee and the DBM/OIT Division of Security and Architecture on an annual basis. A project plan detailing the projects, estimated costs, and estimated completion time required to bring the agency into compliance with the IT Security Policy must be included in the annual report

Information Technology Security Policy Nonpublic Information Standard

- **Agencies shall establish and document a process that protects nonpublic information from disclosure to unauthorized individuals or entities, including other State or federal agencies.**

- **The process shall be compliant with the Maryland Public Information Act and any applicable federal laws.**

Information Technology Security Policy Access Control Standard

- **Authentication**
  - All users must be uniquely identified. Group or shared ids are prohibited unless they are documented as "Functional ids"
  - Password Construction Rules and Change Requirements

- **Authorization**
  - An authorization process which specifically grants access to information ensuring that access is strictly controlled, audited, and that it supports the concepts of "least possible privileges" and " "need-to-know"

Information Technology Security Policy Access Control Standard

Audit Trail

- Events/actions to be logged and kept as required by State and Federal laws/regulations:
  - Additions, changes or deletions to data produced by IT systems
  - An audit trail process to ensure accountability of system and security-related events

Violation Log Management and Review

- The Information Custodian must review all violations within one business day of a discovered occurrence.

Information Technology Security Policy Network Security Standard

Dial-in Access

- Services are prohibited except where they are specifically approved by the Agency CIO:
  - Dial-in desktop modems
  - Use of any type of "remote control" product
  - Use of any network-monitoring tool
- Controls for dial-in users must be implemented:
  - Unique network access user ids different from their application or network user id.
  - A minimum prohibition of answer or pickup until after the sixth (6th) ring
  - Access privileges must be prohibited to any applications except those expressly required (i.e., cannot grant access to entire network, must be application specific)
  - Annual review of access requirements
  - Shall not store data unless the data can be protected from unauthorized access, modification, or destruction

Information Technology Security Policy Network Security Standard

- **Banner Text**
  - The following banner text must be displayed at all system entry points and at all access points to servers, subsystems, etc. where initial user logon occurs

"Access to this system is restricted to authorized users only and limited to approved business purposes. By using this system, you expressly consent to the monitoring of all activities. Any unauthorized access or use of this system is prohibited and could be subject to criminal and civil penalties. All records, reports, e-mail, software, and other data generated by or residing upon this system are the property of State of Maryland and may be used by the State of Maryland for any purpose."

Information Technology Security Policy
Network Security Standard

- **Firewalls & Network Devices**
  - State networks will be protected by firewalls at identified points of interface as determined by system sensitivity and data classification.

- **Intrusion Detection Systems**
  - State networks will be monitored by an IDS implemented at critical junctures. Host-based, network-based, or a combination of both (preferred) may be utilized.

- **Service Interface Agreement**
  - External network connections shall be permitted only after all approvals required by State law are obtained and shall be managed in accordance with a Service Interface Agreement (SIA) that is agreed to by the State agency and the non-State entity.

Information Technology Security Policy Network Security Standard

Teleworking

- An agency must require the same level of security on the microcomputer used at home or offsite as the microcomputer used in the workplace

Mobile Code

- All mobile code or executable content employed within a agency intranet shall be documented in the IT System Security Plan and approved by the Agency CIO

Wireless Networks

- All such networks must at a minimum incorporate the following controls:
  - Properly configuring of routers
  - Encrypting the wireless transmissions using 128 bit (VPNs)
  - Authenticating users with user validation mechanisms(not Passwords)
  - Changing the default service set identifier (SSID)
  - Disabling “broadcast SSID”

Information Technology Security Policy Network Security Standard

- **Private Branch Exchange (PBX)**
  - A single dedicated telephone line that disables access to the public-switched telephone network
  - An automated audit trail
  - Encryption of transmissions
  - Access controls

- **Facsimile**
  - Data transmitted by facsimile must be treated in the same manner as any data communicated by network or PBX based on system sensitivity and data classification

Information Technology Security Policy Physical Security Standard

- **Physical access to IT information processing, storage areas, and storage devices and its supporting infrastructure must be controlled to prevent, detect, and minimize the effects of unauthorized or unintended access to these areas.**

  - **Secured IT Areas**
  - **Storage Media Disposal**
  - **Media Reuse**
  - **Storage And Marking**
  - **Personnel**

Information Technology Security Policy Microcomputer/PC/Laptop Security Standard

- **Agencies must ensure that all microcomputer (i.e., workstation, desktop computers, laptops computers, PDA's, and any other portable device that processes data) are secured against unauthorized access. The level of controls should be commensurate with the information accessed, stored, or processed on these devices.**
  - General Controls
  - Software Licenses And Use
  - Laptop Security And Mobile Computing
  - Personally Owned Data Processing Equipment

Information Technology Security Policy Encryption Standard

- Agencies must ensure that encryption is utilized to protect any non-public information when it is stored or transmitted through any environment.

- IT Systems employing encryption must comply with all applicable Federal Information Processing Standards (FIPS) publications and guidelines for encryption (References located at http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf)

Information Technology Security Policy

IT Information Security Deviation/Risk Acceptance Standard

- **An Information Security Deviation Request/Risk Acceptance form must be completed by the agency if it determines that it cannot or will not comply with the State IT Security Policy. All deviation requests require the approval of the agency CIO, Information Custodian, agency head, and the State CIO**
  - Proposed deviations will be considered on an individual basis
  - Where appropriate, a risk assessment will be performed
  - Requests for deviations must by completed by the requesting Information Custodian and must be made in writing
  - Deviations will be granted for a maximum period of twelve (12) months after which time the deviation will be considered expired

Information Technology Security Policy Use of Electronic Communications Standard

- Applies to information technology security, however, it is not inclusive of other State policies and regulations that may further apply to the use of electronic communications.

- The use of the Internet, E-mail and other State computing equipment, networks and communication facilities is provided to State employees and contract employees as electronic tools to perform their job functions. …

Information Technology Security Policy Use of Electronic Communications Standard

- **Internet and Electronic Communications**
  - Users accessing the Internet or other State electronic communications through State resources may be monitored. Agencies shall develop standards consistent with all State policies and standards regarding E-mail, Internet use, and use of other computer resources.

- **Computer Software Computer Software**
  - Users, unless specifically authorized because of their job functions, are not permitted use unauthorized software

- **IT Incident and Advisories**
  - Each agency shall notify its staff of the personnel designated to provide authenticated notices of IT incidents and advisories

Information Technology Security Policy Standards Self-Assessment Checklist

- **The purpose of this checklist is to assist individuals designing new application, architectures, or modifying existing systems.**
  - The checklist is designed to provide questions pertaining to the majority of the IT Security Standards.
  - It does not include many of the administrative functions detailed in the IT Security Standards and it should not be considered a substitute for reading the IT Security Policy.
  - The checklist had been designed so that an answer of “NO” indicates a potential security issue that requires further investigation.

Information Technology Security Policy Web Location

http://www.dbm.state.md.us

- Featured Links
- Under Technology
  - Policies and Publications

Information Technology Security Policy

Carmella Thompson

Cthompson@dbm.state.md.us

410-260-7663